National Security Education Center

A CONSORTIUM OF LANL INSTITUTES

Information Science and Technology Center Seminar

Ioannis (Yannis) Ch. Paschalidis
Department of Electrical and Computer Engineering
and Division of Systems Engineering
Boston University

"Statistical Anomaly Detection with Applications in Cybersecurity"

Wednesday, March 24, 2010
3:00 - 4:30 PM
TA-3, Bldg. 1690, Room 102 (CNLS Conference Room)

Abstract: Anomaly detection approaches can be broadly grouped into two classes: signature-based detection where known patterns of past anomalies are used to identify ongoing anomalies, and statistical anomaly detection which can accommodate substantial variability in the system activity being monitored and identifies (statistical) patterns that substantially deviate from the normal operation. Earlier work has showed that methods based on pattern matching can always be avoided by sophisticated adversaries, hence, our focus on statistical anomaly detection in this talk.

I will describe a number of methods driven solely from a time-series of system activity data that characterize typical system behavior and identify periods of atypical activity. The latter task relies of identifying statistical deviations from typical activity relies on large deviations techniques we have developed. Our models of typical behavior include i.i.d. and Markovian models both in space and time.

I will describe applications of our techniques in identifying (i) anomalies in Internet traffic and (ii) anomalies in sensor networks reflecting either routing disruptions or anomalies in the physical system being monitored.

Biography: Yannis Paschalidis is a Professor of Electrical & Computer and of Systems Engineering at Boston University, a Co-Director of the Center for Information and Systems Engineering (CISE), and the Academic Director of the Sensor Network Consortium (SNC) -- a industry consortium he spearheaded which currently consists of 14 companies focusing in sensor networks. He obtained a Diploma (1991) from the National Technical University of Athens, and an M.S. (1993) and a Ph.D. (1996) from the Massachusetts Institute of Technology (MIT), all in Electrical Engineering and Computer Science. In September 1996 he joined Boston University where he has been ever since. His current research interests lie in the fields systems and control, networking, applied probability, optimization, operations research, computational biology, and bioinformatics.

Prof. Paschalidis' work on communication networks has been recognized with a CAREER award (2000) from the National Science Foundation and the second prize in the 1997 George E. Nicholson paper competition by INFORMS. He was an invited participant at the 2002 Frontiers of Engineering Symposium, organized by the National Academy of Engineering. His recent work on protein docking has been recognized by a 1st prize in the Protein Interaction Evaluation Meeting (2007) and an invitation to a select workshop at the Institute for Mathematics and Its Applications (IMA) on Molecular and Cellular Biology (2008). He has served in the program/organization committees of many conferences and is an associate editor of Operations Research Letters, the IEEE Transactions on Automatic Control, and the SIAM Journal on Control and Optimization.

Los Alamos NATIONAL LABORATORY EST.1943

Contact the technical host Frank Alexander, fja@lanl.gov, 665-4518 for further information.
——Hosted by the Information Science and Technology Center (ISTC)——